REMARKS

Following is information requested by the Examiner in the paper mailed December 23, 2003. Such information has been itemized by paragraph per the paper mailed December 23, 2003.

2. The Examiner has requested that applicant identify products and services embodying the disclosed subject matter of Claims 1-29, and identify the properties of similar products and services found in the prior art. In response, applicant submits herewith Appendix A including a description of the "AirMagnet Wireless LAN Handheld Analyzer," which is a product embodying the subject matter of applicant's claims. The properties of similar products/services that are found in the prior art are either unknown or cannot be readily obtained.

3. The Examiner has further requested that applicant provide the names of any products or services that have incorporated the claimed subject matter. Again, in response, applicant submits herewith Appendix A including a description of a product named "AirMagnet Wireless LAN Handheld Analyzer," which has incorporated the claimed subject matter.

4. The Examiner has further requested a copy of the rigid comparison of the alleged infringing device and method identified in the petition filed on 06/02/03 (paper #5) along with any supporting documents concerning place and date(s) of use and/or sale of the alleged infringing device. In response, applicant submits herewith Appendix B including a claim chart correlating the infringing device and method of Appendix A with the claims of the present application. With respect to the requested supporting documents concerning place and date(s) of use and/or sale of the alleged infringing

device, Appendix A indicates that the subject matter relating to the "AirMagnet Wireless LAN Handheld Analyzer" was published in 08/02.

5. The Examiner has still further requested that applicant state the specific improvements of the claimed subject matter in Claims 1-29 over the disclosed prior art and indicate the specific elements in the claimed subject matter that provide those improvements. In response, following is such claim-by-claim analysis.

Claims 1-29 provide a technique for reporting on network analysis. To this end, the network traffic information is capable of being reported in a distributed environment. Shown below in **bold** arc selected elements in the claimed subject matter that provide these improvements.

1. A method for reporting on network analysis, comprising:

(a) **collecting network traffic information utilizing a plurality of agents installed in computers distributed among a plurality of zones;**

(b) **receiving the network traffic information collected from the agents associated with each zone at a separate controller**; and

(c) **transmitting a report on the network traffic information from the controller to a computer coupled thereto via a network.**

2. The method as recited in claim 1, wherein **the report is capable of being displayed on the computer utilizing a network browser.**

3. The method as recited in claim 1, wherein the network includes the Internet.

4. The method as recited in claim 1, and further comprising **receiving a request at one of the controllers for a report on the network traffic information corresponding to the zone associated with the controller.**

5. The method as recited in claim 4, wherein **the report is transmitted in response to the request.**

6. The method as recited in claim 1, wherein **the report includes a network analyzer report.**

7. The method as recited in claim 1, wherein **the report includes a plurality of objects.**

8. The method as recited in claim 7, wherein **the objects are in a tree representation.**

9. A computer program product for reporting on network analysis, comprising:

(a) computer code for **collecting network traffic information utilizing a plurality of agents installed in computers distributed among a plurality of zones;**

(b) computer code for **receiving the network traffic information collected from the agents associated with each zone at a separate controller**; and

(c) computer code for **transmitting a report on the network traffic information from the controller to a computer coupled thereto via a network.**

10. The computer program product as recited in claim 9, wherein **the report is capable of being displayed on the computer utilizing a network browser.**

11. The computer program product as recited in claim 9, wherein the network includes the Internet.

12. The computer program product as recited in claim 9, and further comprising **receiving a request at one of the controllers for a report on the network traffic information corresponding to the zone associated with the controller.**

13. The computer program product as recited in claim 12, wherein **the report is transmitted in response to the request.**

14. The computer program product as recited in claim 9, wherein **the report includes a network analyzer report.**

15. The computer program product as recited in claim 9, wherein **the report includes a plurality of objects.**

16. The computer program product as recited in claim 15, wherein **the objects are in a tree representation.**

17. A system for reporting on network analysis, comprising:
(a) logic for **collecting network traffic information utilizing a plurality of agents installed in computers distributed among a plurality of zones;**
(b) logic for **receiving the network traffic information collected from the agents associated with each zone at a separate controller**; and
(c) logic for **transmitting a report on the network traffic information from the controller to a computer coupled thereto via a network.**

18. The system as recited in claim 17, wherein **the report is capable of being displayed on the computer utilizing a network browser.**

19. The system as recited in claim 17, wherein the network includes the Internet.

20. The system as recited in claim 17, and further comprising **receiving a request at one of the controllers for a report on the network traffic information corresponding to the zone associated with the controller.**

21. The system as recited in claim 20, wherein **the report is transmitted in response to the request.**

22. The system as recited in claim 17, wherein **the report includes a network analyzer report.**

23. The system as recited in claim 17, wherein **the report includes a plurality of objects.**

24. The system as recited in claim 23, wherein **the objects are in a tree representation.**

25. A method for reporting on network analysis, comprising:

(a) **collecting network traffic information utilizing a plurality of agents installed in computers distributed among a plurality of zones;**

(b) **receiving the network traffic information collected from the agents associated with each zone at a separate controller;**

(c) **receiving a request at one of the controllers for a report on the network traffic information corresponding to the zone associated with the controller;** and

(d) **transmitting the report from the controller to a computer coupled thereto via a network;**

(e) **wherein the report is capable of being displayed on the computer utilizing a network browser.**

26. A method for reporting on network analysis, comprising:

collecting network traffic information utilizing a plurality of information collectors installed in computers distributed among a plurality of zones;

receiving the network traffic information collected from the information collectors associated with each zone at an information collector manager; and

generating a report on the network traffic information associated with a selected one of the zones.

27. The method as recited in claim 26, wherein **the information relates to wireless network traffic.**

28. A computer program product for reporting on network analysis, comprising:

computer code for **collecting network traffic information utilizing a plurality of information collectors installed in computers distributed among a plurality of zones;**

computer code for **receiving the network traffic information collected from the information collectors associated with each zone at an information collector manager**; and

computer code for **generating a report on the network traffic information associated with a selected one of the zones.**

29. The computer program product as recited in claim 28, wherein **the information relates to wireless network traffic.**

The Examiner continues by stating that the information disclosure statement filed February 12, 2002 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP 609 because no explanation of the relevance to the present application has been provided. In response, applicant draws the Examiner's attention to the following excerpt from MPEP 609 A(3), wherein it states that such concise explanation is required only for non-English submissions. Thus, applicant asserts that the information disclosure statement filed February 12, 2002 indeed complies with the provisions of 37 CFR 1.97, 1.98 and MPEP 609, and should be considered by the Examiner.

> "A (3) Concise Explanation of Relevance
>
> Each information disclosure statement must further include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent, publication, or other information listed that is not in the English language. The concise explanation may be either separate from the specification or incorporated therein. The requirement for a concise explanation of relevance is limited to information that is not in the English language."

Still yet, the Examiner has rejected Claims 1-26 and 28 under 35 U.S.C. 102(b) as being anticipated by Fletcher et al., USPN 6,108,782. Still yet, the Examiner has rejected Claims 27 and 29 under 35 U.S.C. 103(a) as being unpatentable over Fletcher in view of Sharon et al., USPN 6,137,782.

Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove. For example, the Examiner relies on the following excerpt of Fletcher to make a prior art showing of applicant's claimed "wherein the report includes a plurality of objects in a tree representation" (note all independent claims).

> "SNMP is designed to support the exchange of Management Information Base (MIB) objects through use of two simple verbs, get and set. MIB objects can be control structures, such as a retry counter in an adaptor. Get can get the current value of the MIB and set can change it." (col. 3, lines 47-49)

> "The dRMON Collector receives RMON analysis and capture data from the agents and sorts, collates, and aggregates that information into a cohesive database that recreates the view a prior art RMON probe would have if the ESs were all on the same LAN segment with the prior art probe. The collector can then makes this information available to management applications, either using SNMP and the MIB-II and RMON MIBs or optionally, to WEB browsers via HTTP or other web interface language. Different instances of the Collector, like the Agent, can be developed to support a number of different operating systems." (col. 9, lines 33-43)

After carefully reviewing such excerpt along with the remaining Fletcher reference, it appears to applicant that the Examiner is not taking into consideration the full weight of applicant's claims. Specifically, there is simply no disclosure, teaching or suggestion of a "report [that] includes a plurality of objects in a tree representation," as claimed by applicant. Only applicant teaches and claims such a novel tree-representation-based report for morc effectively displaying objects and reporting on the same.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criteria has simply not been met by the Fletcher reference.

Nevertheless, in the spirit of expediting the prosecution of the present application by further distinguishing applicant's claimed invention, applicant has amended each of the independent claims to recite "a plurality of consoles [that] are coupled to the information collector manager, controller, etc. for collecting the network traffic information from the information collector manager, controller, etc. and displaying the network traffic information from the information collector manager, controller, etc., wherein a user interface is adapted for analyzing an output."

Still yet, further claimed in combination with the foregoing features are "intrusion detection services [provided]... based on the network traffic information." Again, see all of the independent claims.

Such limitations provide not only a unique combination of features and components, but also work synergistically to provide an improved system. For example, by utilizing the specific features for not only quality assurance, but also intrusion detection, the present system is ideally equipped for distributed network analysis of highly vulnerable networks, where security is particularly problematic.

Still yet, by providing a three-tier approach including "information collectors" (i.e. agents, etc.) communicating with at least one "information collector manager" (i.e. controller, etc.) communicating, in turn, with "consoles", an improved distributed network analysis approach is provided where access to reporting is improved. Simply nowhere in the prior art is there such a combination of features and components for fulfilling the foregoing objectives. For example, note that only one management console 54 (see FIG. 1) is disclosed by Fletcher.

A specific showing of each of the foregoing limitations or a notice of allowance is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P064_01.306.01).

Respectfully submitted,
Silicon Valley IP Group

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100

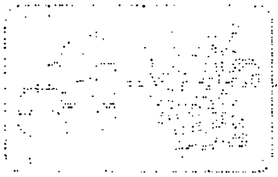
Appendix A

The AIRMAGNET

Distributed WLAN Integrity Management System

The past year has seen the role of the Wireless LAN in the enterprise undergo a fundamental transformation. A groundswell of demand from both CXOs and end-users alike has made Wi-Fi a pervasive component of the enterprise network. This adoption, however, has been anything but strict. Growth has been notoriously viral and unregulated, making it a challenge to even know about all the Wi-Fi infrastructure being deployed, much less manage it.

New breeds of security measures have evolved out of necessity, but have done so without a methodology to insure that they are actually enforced. Environmental factors continue to impact the performance and reliability of the network itself, and a reliance on outdated tools intended for wired networks has forced network managers into a purely reactive management strategy. These issues are the unique domain of the AirMagnet Distributed System.

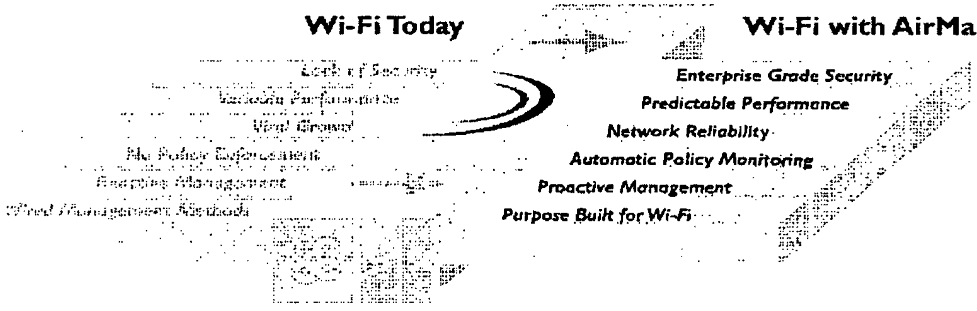


The AirMagnet Distributed System

The AirMagnet Distributed System is the first and only solution to fully address the Integrity of wireless networks - providing 24x7 monitoring of the Security, Performance, and Reliability of any number of WLANs, and delivering actionable information to management staffs and systems anywhere in the world.

AirMagnet Distributed replaces an informational void with complete knowledge of every Wi-Fi device and channel in the environment regardless of band (11a, 11b, or 11g). Management staff can easily monitor the security measures in use on every device to insure compliance with established policies, while automatically scanning for dozens of wireless network attacks. In addition to security, the AirMagnet Distributed System proactively addresses the performance and reliability of the network, without which, the WLAN simply could not be held to enterprise standards. Dozens of configurable alarms proactively alert managers to developing issues before they lead to problems, and a suite of active testing utilities enable managers to test their infrastructure from any location they choose.

WLAN
Integrity
Management
ensuring network
Security
Performance
and Reliability



Wi-Fi Today

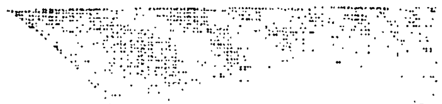
Lack of Security
Variable Performance
Viral Growth
No Policy Enforcement
Reactive Management
Wired Management Methods

Wi-Fi with AirMagnet

Enterprise Grade Security
Predictable Performance
Network Reliability
Automatic Policy Monitoring
Proactive Management
Purpose Built for Wi-Fi

AirMagnet Distributed

WLAN Integrity Management delivers security, performance, and reliability throughout the network lifecycle



AirMagnet Distributed: The Industry's Most Sophisticated Monitoring

The front line of the AirMagnet Distributed System is manned by strategically placed Intelligent Sensors. These sensors provide around-the-clock coverage of the entire wireless environment including all 11a, 11b, and 11g channels and infrastructure. Each individual sensor is armed with the patent-pending AirWISE Analytical Engine, to autonomously monitor the security, performance, and reliability of the network. Functionality built into each sensor, allows network professionals to:

Gain Control Over Security Policy

No issue has defined Wi-Fi more than security. While the past year has welcomed new security protocols that make WLANs as secure as their wired counterparts, insuring that all users and stations comply with these security measures has been another issue entirely. AirMagnet Sensors address this gap by auditing and validating the security of every Wi-Fi device in the network, providing managers with an easy process to insure all users employ the appropriate level of security. Supported protocols include:

- wep
- leap
- peap
- tkip
- mic
- 802.1x
- ttls
- tls
- wpa
- pptp vpn
- l2tp vpn
- ssh vpn
- ipsec vpn

Detect Wireless Intruders and Attacks

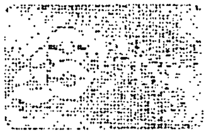
Maintaining internal defenses is only half the security battle. As Wi-Fi has grown, so too have the number and sophistication of wireless attacks. AirMagnet Sensors have been engineered specifically to counter these threats - scanning the environment for Rogue APs and War-Drivers, Spoofed MAC Addresses, and a host of Denial of Service Attacks unique to Wi-Fi. Sensors send encrypted real-time alarms in response to an attack , allowing staff to respond before the network is impacted.

Lock In Network Performance

Radio Frequency transmissions are inherently susceptible to environmental factors such as physical obstructions and radio interference from a variety of sources. If not identified and managed, these factors can lead to unacceptable performance for the end-user. To address this challenge, AirMagnet Sensors constantly monitor and alarm on over 20 key indicators of network health, allowing engineers to take a proactive approach to the maintenance of the network.

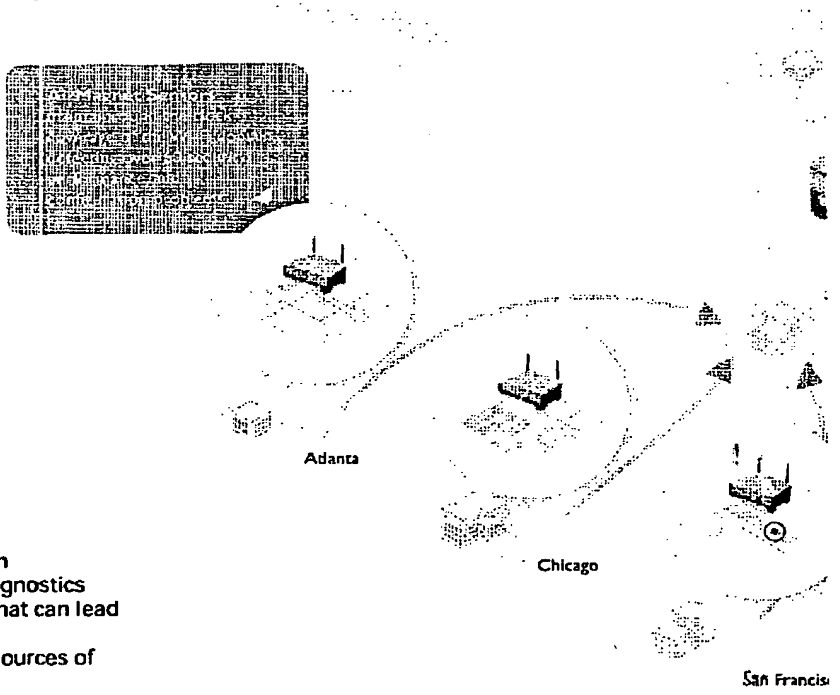
Ensure Network Reliability

In addition to predictable performance, WLANs must be highly reliable before being considered business grade. The AirMagnet Distributed System addresses this need with a suite of alarms and diagnostics that detect network faults and misconfigurations that can lead to outages in the network. These diagnostics are compl mented by active utilities to pin down the sources of connectivity problems in the network.



AirMagnet Distributed: 24x7 Wi-Fi Integrity Management

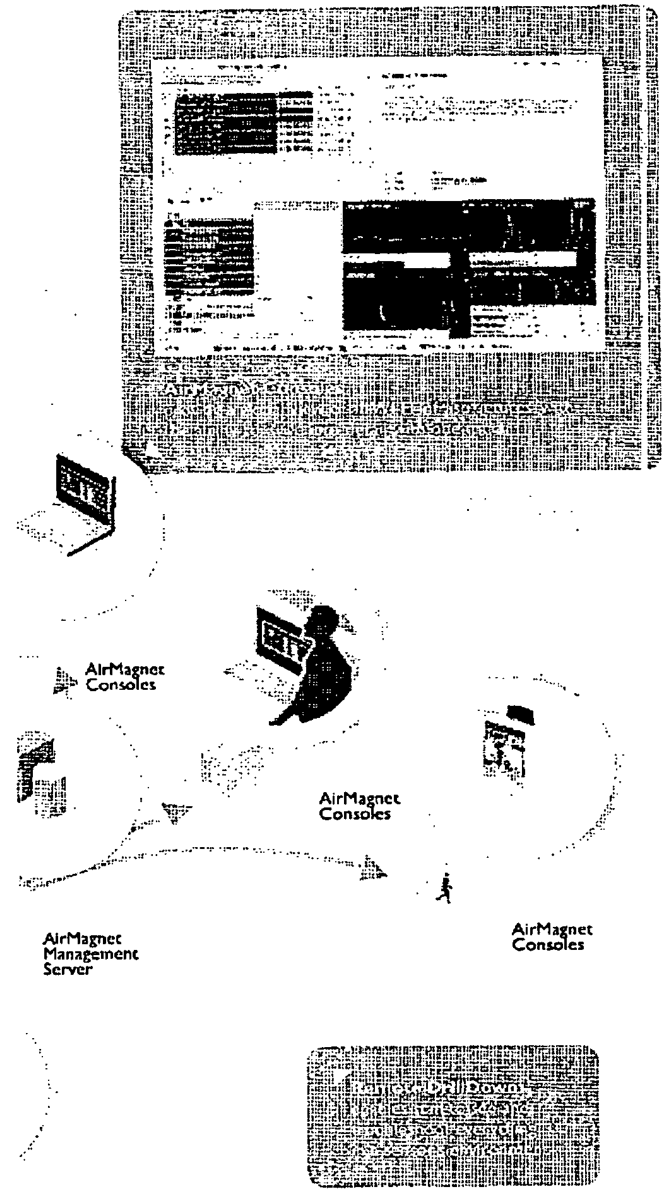
- multi-band coverage - 11 a,b,g
- infrastructure agnostic
- standards based security
- control over network policy and growth
- proactive management
- local processing ensures enterprise scalability
- integrated with leading network management consoles



Secure Scalable Management

Contr lled Centralized System Management

The AirMagnet Management Server receives information from every AirMagnet Sensor and provides a centralized SQL database of all network data and alarms. SNMP traps allow for seemless integration with leading management consoles such as HP Open View and CA UniCenter. All traffic is secured via SSL and TLS insuring management information remains secure while interoperating with corporate firewalls and VPNs.



Configuration and User Management

The Management Server also maintains configurations for every Sensor in the System, allowing IT Personnel to tune sensor thresholds appropriately for each location. Additionally, AirMagnet Distributed supports three unique user levels, insuring that the users access only the level of information appropriate for their role and level of responsibility.

Anywhere, Anytime Integrity Management

The AirMagnet Management Console provides the User Interface to The AirMagnet Distributed System. From the Management Console, Users can view alarms and WLAN health by Campus, Building, Floor, or by individual Sensor. Consoles can be run securely whether in a NOC, or remotely on a laptop or Pocket PC - keeping networkers connected to the information they need, regardless of their location.

Remote Drill-Down

One of the most powerful features of the AirMagnet Console is the ability to remotely drill in to any AirMagnet Sensor. This allows Users to securely connect to a particular sensor, from any location, and view detailed information in real-time. Users can view low level data on every channel and device in the area, see alarms, real-time local statistics, and even review packet decodes.

Remote Troubleshooting and Active Tools

Using the Remote UI built into the AirMagnet Management Console, Users can leverage a host of active troubleshooting tools to pinpoint problems in the network. These tools allow the User to remotely test Throughput on a particular AP, Diagnose Connection Problems, and perform Layer 3 Debugging and End-to-End Provisioning. Such remote capability greatly reduces the need to dispatch resources when troubleshooting the WLAN.

Efficient Use of Network Resources

Most remote monitoring systems simply capture wireless packets and resend them to a remote site for processing, needlessly consuming valuable bandwidth. AirMagnet Sensors, conversely process locally, sending real-time alarms only when thresholds are reached. Trending data is saved on the sensor, and securely sent at regular intervals t the Management Server, minimizing operational l ad on the network and servers.

The Comprehensive Solution

AirMagnet Distributed Specifications

General

Supported 802.11 Standards	A, B, G
Radio Frequency	2.4 GHz, 5 GHz Bands Concurrently
Supported Security Standards	802.1x, LEAP, TKIP, MIC, PEAP, WPA, VPNs
SNMP Traps	Yes
Integration to 3rd Party Consoles	HP OpenView, CA Unicenter
Reporter Option	Yes
Secure Communication	SSL, TLS
Real-Time Decode	Yes
Decode Level	Layers 1,2,3
Trace File Compatiblity	AirMagnet, Sniffer, Ethereal

AirMagnet, Inc.
465 Fairchild Drive,
Suite 203
Mountain View, CA
94043
650-694-6754
www.AirMagnet.com
info@airmagnet.com

Security Management

Policy Enforcement - Detects 15 Violations

- AP with WEP Disabled
- Client Station with WEP Disabled
- WEP IV Reused
- Device Using Open Authentication
- AP Unconfigured
- Rogue AP
- Rogue Client Station
- Crackable WEP IV In Use
- Device Unprotected by VPN
- Device Unprotected by 802.1x
- AP Broadcasting SSID
- Ad-hoc Station Detected
- Long EAPRekey Timeout
- Device Using Shared Key Authentication
- Unassociated Station Detected

Intrusion Detection - Detects 16 Threats

- Spoofed MAC Address Detected
- Device Probing With NULL SSID
- Dictionary Attack in EAP Methods
- Abnormal Authentication Failures
- Denial of Service Attacks
  - Association Flood
  - Authentication Flood
  - EAPOL logoff
  - EAPOL start
  - EAPOL ID Flood
  - EAPOL Spoofed Success
  - Deauthentication Broadcast
  - Deauthentication Flood
  - Dis-association Broadcast
  - Dis-association Flood
  - RF Jamming

End to End Connectivity

- Mismatched SSID
- Client with Match All SSID
- Mismatched RF Channel
- Mismatched Privacy Setting
- Authentication Failure
- Reassociation Failure
- Possible Equipment Failure
- AP Signal Out of Range
- Mismatched Capability Settings
- Device With Bad WEP Key
- Higher Layer Protocol Problem
- 802.1x Authentication Failure

Tools

- Perform
- DHCP
- Ping
- TraceRoute
- Whois

Performance Management

Detects 12 Sources of Poor Performance

- AP With Weak Signal Strength
- Low Transmission Speed
- High Packet Fragmentation Rate
- High Bandwith Usage
- Missed AP Beacons
- High Speed Transmission Not Supported
- Channel Overloaded by APs
- 802.11 Performance Options Not Supported
- APs With Mutual Interference
- High Mgmt and Control Frame Overhead
- AP Overloaded with Clients
- AP Overloaded by Bandwith Consumption

Reliability Management

Detects 13 Sources of Poor Reliability

- WLAN Hidden Node Problem
- AP System of Firmware Reset
- Station Excessively Switching Between APs
- Packet Error Rate Exceeded
- AP Association Capacity Full
- Channel with Overloaded APs
- DCF and PCF Controls Active at Same Time
- Conflicting AP Configuration
- Channel with High Noise Levels
- High Multicast/Broadcast Traffic
- Ad-hoc Station Using AP SSID
- Station Constantly Probing for Connection

Software Sensor

Operating System	Windows 2000, XP (PC Not Included)
Memory	128 MB Minimum
Disk Storage	20 MB Free Space Minimum
Supported 802.11 PC or PCI Cards	Cisco PCM352, LMC352, PCI352, NetGear WAB501

Appliance Sensor

Operating System	Embedded Linux (Hardware Included)
Memory	64 MB
Antenna	Omni-directional, 2.4 GHz: 3.0 dbi, 5.25 GHz: 5.5 dbi, 5.75 GHz: 5.0 dbi
802.11 Radio Card	Atheros based a/b/g multi-mode card
10/100 Ethernet Port	2 With Power Over Ethernet Option

Management Server

Operating System	Windows 2000, XP (PC Not Included)
CPU	800MHz Minimum
Memory	256 MB Minimum
Disk Storage	4 GB Free Space
# Of Sensors Supported	Unlimited
Information Repository	Aggregate Sensor Alarms, wireless device and traffic trends

Management Console

Operating System	Windows 2000, XP (PC Not Included)
CPU	800 MHz Minimum
Memory	256 MB Minimum
Disk Storage	20 MB Free Space Minimum

AIRMAGNET

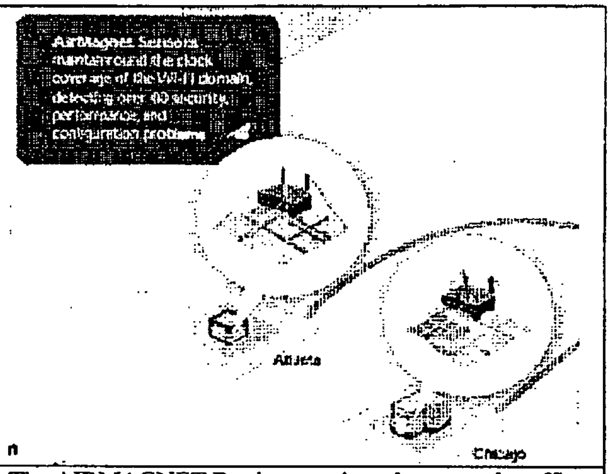
APPENDIX B

INVESTIGATION OF U.S. PATENT APP. SER. NO. 10/029,687

Claims 26 & 28 of U.S. Patent App. Ser. No. 10/029,687	AIRMAGNET Distributed WLAN Integrity Management System
26. A method for reporting on network analysis, comprising:	The AIRMAGNET Product includes a method for reporting on network analysis. See excerpt(s) below. "Each individual sensor is armed with the patent-pending AirWISE Analytical Engine, to autonomously monitor the security, performance, and reliability of the network." See Page 2 of Appendix A.
collecting network traffic information utilizing a plurality of information collectors installed in computers distributed among a plurality of zones;	The AIRMAGNET Product collects network traffic information utilizing a plurality of information collectors installed in computers distributed among a plurality of zones. See excerpt(s) below. **"Controlled Centralized System Management** The AirMagnet Management Server receives information from every AirMagnet Sensor and provides a centralized SQL database of all network data and alarms. SNMP traps allow for seemless integration with leading management consoles such as HP Open View and CA UniCenter. All traffic is secured via SSL and TLS insuring management information remains secure while interoperating with corporate firewalls and VPNs. **Configuration and User Management** The Management Server also maintains configurations for every Sensor in the System, allowing IT Personnel to tune sensor thresholds appropriately for each location. Additionally, AirMagnet Distributed supports three unique user levels, insuring that the users access only the level of information appropriate." See Page 3 of Appendix A. See Figure below from Page 2 of Appendix A.

APPENDIX B

INVESTIGATION OF U.S. PATENT APP. SER. NO. 10/029,687

Claims 26 & 28 of U.S. Patent App. Ser. No. 10/029,687	AIRMAGNET Distributed WLAN Integrity Management System
	 AirMagnet Sensors maintain round the clock coverage of the Wi-Fi domain, detecting over 40 security, performance, and configuration problems Atlanta Chicago
receiving the network traffic information collected from the information collectors associated with each zone at an information collector manager; and	The AIRMAGNET Product receives the network traffic information collected from the information collectors associated with each zone at an information collector manager. See excerpt(s) below. **"Controlled Centralized System Management** The AirMagnet Management Server receives information from every AirMagnet Sensor and provides a centralized SQL database of all network data and alarms. SNMP traps allow for seemless integration with leading management consoles such as HP Open View and CA UniCenter. All traffic is secured via SSL and TLS insuring management information remains secure while interoperating with corporate firewalls and VPNs. **Configuration and User Management** The Management Server also maintains configurations for every Sensor in the System, allowing IT Personnel to tune sensor thresholds appropriately for each location. Additionally, AirMagnet Distributed supports three unique user levels, insuring that the users access only the level of information appropriate." See Page 3 of Appendix A.

APPENDIX B

INVESTIGATION OF U.S. PATENT APP. SER. NO. 10/029,687

Claims 26 & 28 of U.S. Patent App. Ser. No. 10/029,687	AIRMAGNET Distributed WLAN Integrity Management System
generating a report on the network traffic information associated with a selected one of the zones.	The AIRMAGNET Product generates a report on the network traffic information associated with a selected one of the zones. See excerpt(s) below. **"Remote Drill-Down** One of the most powerful features of the AirMagnet Console is the ability to remotely drill in to any AirMagnet Sensor. This allows Users to securely connect to a particular sensor, from any location, and view detailed information in real-time. Users can view low level data on every channel and device in the area, see alarms, real-time local statistics, and even review packet decodes." See Page 3 of Appendix A.
28. A computer program product for reporting on network analysis, comprising: computer code for collecting network traffic information utilizing a plurality of information collectors installed in computers distributed among a plurality of zones; computer code for receiving the network traffic information collected from the information collectors associated with each zone at an information collector manager; and computer code for generating a report on the network traffic information associated with a selected one of the zones.	Claim 28 is the software analog to Claim 26. The AIRMAGNET Product includes a computer program product for reporting on network analysis, as set forth in Claim 26. See excerpts above.